CWC IIT User Agreement

Schedule II

DATA PROTECTION ADDENDUM

This Data Processing Addendum forms part of the Agreement between CWC ("**Processor**") and ("NPO")(**collectively**, the "**Parties**").

1. DEFINITIONS

1.1. In this Data Protection Addendum capitalised terms have the same meanings as in the Agreement. In addition, the following definitions have the meanings given below with respect to this Data Protection Addendum ("DPA"):

1.1.1. ACE Agreements means the Agreement between CWC and ACE for the provision of a Customer Insight Toolkit (reference ACE 073 ITT) ("**ACE-CWC Agreement**"), which sets out the purpose, terms, conditions and specifications for provision of the IIT and IIT Services to NPOs, including terms related to data protection and the Funding Agreement between the NPO and ACE, which sets the parameters for NPO use of the IIT and IIT Services and imposes reporting and processing obligations on NPOs which includes access to underlying Personal Data;

1.1.2. Appropriate Safeguards means the mechanism(s) permitting international transfers of Personal Data specified in Chapter V of the GDPR and applicable DP Law, including Adequacy (as defined in DP Law) and Standard Contractual Clauses;

1.1.3. Controller, Data Importer, Data Exporter, Data Subject, International Organisation, Personal Data, Personal Data Breach, Processor and **processing** shall have the respective meanings given to them in applicable Data Protection Law (and related expressions, including **process, processed, processing,** and **processes** shall be construed accordingly);

1.1.4. Data Privacy Notice means the information Controllers are required to communicate to Data Subjects under DP Law, the content and manner of communicating it as specified in Arts. 12 to 14, GDPR and as extended or amended or further addressed in applicable DP Law;

1.1.5. Data Protection Law or DP Law means, as applicable and binding on the NPO, the Processor and/or the IIT, all legislation and regulatory requirements in force from time to time relating to the use of Personal Data and the privacy of electronic communications, including without limitation:

(a) the General Data Protection Regulation ((EU) 2016/679) ("**GDPR**"), any other directly applicable European Union regulation giving effect to or corresponding with or implementing any of the GDPR and Directive 2002/58/EC (the ePrivacy Directive) (for so long as and to the extent that the law of the European Union has legal effect in the UK) as may be replaced by any equivalent UK legislation;

(b) any laws which implement any such laws, including any data protection legislation from time to time in force in the UK including the **UK Data Protection Act 2018** ("UK DPA 2018"), the UK Privacy and Electronic Communications Regulations (EC Directive) 2003 (as amended from time to time) ("**UK PECR**") or any successor or implementing legislation;

(c) any Applicable Laws replacing, amending, extending, re-enacting or consolidating any of the above Data Protection Laws from time to time;

1.1.6. Data Protection Losses means all liabilities, including all:

(a) costs (including legal costs), claims, demands, actions, settlements, interest, charges, procedures, expenses, losses and damages (including relating to material or non-material damage); and

(b) to the extent permitted by Applicable Law: administrative fines, penalties, sanctions, liabilities or other remedies imposed by a Supervisory Authority; compensation which is ordered by a Supervisory Authority to be paid to a Data Subject; and the reasonable costs of compliance with investigations by a Supervisory Authority.

1.1.7. Data Subject Request ("**DSR**") means a request made by a Data Subject to exercise any rights of Data Subjects under Data Protection Laws with respect to Personal Data that we process on your behalf as described in Chapter III of the GDPR (as modified or extended in any applicable DP Law). This includes, but is not limited to, the right to erase or correct Personal Data, the right to portability, and the right to object to direct marketing;

1.1.8. International Data Transfer means the transfer of Protected Data from within the European Economic Area out of the European Economic Area or from the United Kingdom to a country outside the United Kingdom, which would be prohibited by DP Law in the absence of Appropriate Safeguards;

1.1.9. List of Sub-Processors means the latest version of the list of Sub-Processors we use, as updated from time to time, which as at the time of signing are listed in Annex C (List of Sub-Processors) to this DPA

1.1.10. Mandated Data means data collected or generated by the NPO using the IIT that ACE may access directly from CWC pursuant to clause 10 of the Funding Agreement and which may include Personal Data. Mandated Data includes responses to the quality metric statements, basic demographic information from NPO audiences, meta-data relating to the event evaluated and any other agreed fields but excludes responses to bespoke questions NPOs choose to ask or Personal Data;

1.1.11. Participant means Data Subjects who have participated in a Survey;

1.1.12. Participant Communication means the content of a message of any medium you convey to or make available to a Participant in connection with the Survey. For greater certainty, it does not include any communications unrelated to the Survey or the use of the IIT such as promotional material, marketing emails, etc;

1.1.13. Processing Instructions has the meaning given to that term in clause 6;

1.1.14. Protected Data means Personal Data which you have provided to us, that we have received on your behalf, or that you process in connection with the IIT or the performance of our obligations under the Agreement or the DPA, but excludes Mandated Data;

1.1.15. Standard Contractual Clauses means the standard data protection clauses for the transfer of Personal Data from the European Economic Area to Data Processors established in third countries as set out in the Annex to European Commission Decision 2010/87/EU (or any subsequent clauses approved by the European Commission or the relevant Supervisory Authority pursuant to Arts. 46(2)(c) and (d) of the GDPR or equivalent under DP Law that may amend or supersede such standard contractual clauses);

1.1.16. Sub-Processor means any agent, subcontractor or other third party (excluding its employees)] engaged by us for carrying out any processing activities on your behalf in respect of the Protected Data;

1.1.17. Supervisory Authority means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering Data Protection Laws and, in the UK means the Information Commissioner's Office ("**ICO**") ;

1.1.18. We, us, our means or refers to CWC;

1.1.19. You, your, yours means or refers to the natural person or legal entity named as NPO in the Agreement and this DPA.

2. RELATIONSHIP WITH THE AGREEMENT AND RELATED DOCUMENTS

2.1. Scope. This DPA only applies to the extent that the processing relates to or is in connection with Protected Data to which DP Law applies. For greater certainty, this applies to processing of the Personal Data of Survey Participants and Authorised Users in the UK under the Agreement and as further set out in Annex A to this DPA. Prior DPAs. This DPA supersedes any prior DPA between the Parties related to the IIT.

2.2. No third-party rights. No one other than the Parties or their successors or permitted assignees shall have any rights under this DPA.

2.3. Exception. Notwithstanding clause 2.4, the Parties acknowledge and agree that ACE shall have such rights under this DPA and the Parties shall have such obligations towards ACE as are required to give effect to the ACE's rights under the ACE Agreements. This includes Ace's right to access Mandated Data directly from CWC as stipulated in clause 10 of the Funding Agreement.

2.4. Governing Law. This DPA shall be governed by and interpreted in accordance with the governing law and jurisdiction applicable to the Agreement.

2.5. Survival. This DPA (as updated from time to time) shall survive termination (for any reason) or expiry of the Agreement and continue until no Protected Data remains in the possession or control of the Processor or any Sub-Processor, except that clause 13 (Deletion of Protected Data) and 14 (Indemnity) shall continue indefinitely.

3. COMPLIANCE WITH DATA PROTECTION LAW AND RELATIONSHIP OF THE PARTIES

3.1. Compliance with Data Protection Law. The Parties acknowledge and agree to comply with the Data Protection Laws as applicable to the Personal Data they process in relation to the Agreement and in connection with the IIT and IIT Services. Nothing in this DPA relieves either party of any responsibilities or liabilities under DP Law.

3.2. Processor and Controller. The Parties agree that, for the Protected Data, you (the NPO) are the Controller and CWC is the Processor.

3.3. Exception – CWC as Controller. The Parties acknowledge and agree that CWC is a Controller for Personal Data that it processes for the purposes of its own business and in the administration of the Agreement. Such Personal Data shall be limited to the business contact information of NPO personnel responsible for administering the Agreement and to the minimum extent necessary to provide the Services (including session cookies and load-balancing cookies dropped on Authorised Users' devices to ensure the pages function properly; audit logs for security purposes and to document Processing Instructions; IP addresses for security and Survey integrity reasons). We undertake to treat such Personal Data as confidential and process it in accordance with CWC's Data Privacy Notice as updated from time to time.

3.4. Registrations and notification requirements. The Parties undertake to fulfil any registration or notification requirements with the relevant Supervisory Authorities. CWC is registered as a Controller under ICO registration number ZA141427.

4. YOUR DATA PROCESSING OBLIGATIONS

4.1. You shall at all times comply with all applicable DP Laws in connection with the processing of Protected Data and the use of the IIT and IIT Services and ensure all Processing Instructions in respect of Protected Data (including the terms of this Agreement) comply at all times with DP Law.

4.2. For greater certainty, you warrant, represent and undertake, that at all times:

4.2.1. Lawful Processing. All Protected Data (if processed in accordance with our Agreement) complies in all respects with DP Law, specifically but not limited to:

(a) Mandatory NPO Data Privacy Notice. You have and will clearly post, maintain, and abide by a publicly accessible Data Privacy Notice that describes your use of Protected Data processed using the IIT and shall include a link to the ACE IIT Privacy Policy https://impactandinsight.co.uk/privacy-policy/. In addition, you may, at your option, include our Recommended Processor Privacy Statement in Annex D (Recommended Processor Privacy Statement) to this DPA to describe how we process Protected Data on your behalf;

(b) Mandatory Cookie Notice and Consents. You will provide and obtain all Data Privacy Notices and obtain all necessary consents required by applicable DP Law to enable us to use cookies and similar tracking technologies (like web beacons or pixels) lawfully on and collect data from the devices of Survey Participants where applicable and Authorised Users of the IIT in accordance with and as described in our Cookie Statement https://impactandinsight.co.uk/cookie-policy/; You may use the Recommended Cookie Statement in Annex D (Recommended Processor Privacy Statements);

4.2.2. Agents and employees. You shall ensure that you or any agents, employees, contractors or other Authorised Users comply with all DP Laws in connection with the Protected Data and the IIT and the foregoing obligations;

4.2.3. You have undertaken due diligence in relation to our processing operations and commitments and you are satisfied (and all times that you continue to use the IIT remain satisfied) that:

(a) Our processing operations are suitable for your purposes with respect to processing the Protected Data;

(b) The technical and organisational measures set out in Annex B (Technical and Organisational Security Measures) to this DPA (as updated from time to time) ensure a level of security appropriate to the risk with respect to the Protected Data if we comply with them; and

(c) We have sufficient expertise, reliability and resources to implement technical and organisational measures that meet the requirements of DP Laws.

5. OUR DATA PROCESSING OBLIGATIONS

5.1. We shall process Protected Data in compliance with our obligations under DP Laws and the terms of this DPA and the Agreement.

5.2. We undertake to process Protected Data only in accordance with Processing Instructions and not to make any use of Protected Data except as required to provide or support the IIT or IIT Services unless:

5.2.1. Alternative Processing Instructions are agreed between the Parties in accordance with the requirements in clause 6 (Processing Instructions);

5.2.2. We are required or permitted to do otherwise by Applicable Law, in which case we shall notify you of any such requirement before processing the Protected Data (except where Applicable Law prohibits such information on important grounds of public interest);

5.2.3. We believe a Processing Instruction infringes Data Protection Law, in which case we shall promptly inform you of this. In such cases we reserve the right to cease to provide any or all of the relevant IIT until the Parties have agreed appropriate amended Processing Instructions which are not infringing;

5.2.4. The processing is required for our own purposes as a Controller as described in our Data Privacy Notice, in which case we undertake to take measures to minimise the use of and/or restrict access to the Protected Data as appropriate to ensure any such processing is necessary and proportionate; or

5.2.5. You have given us prior written approval to use it for our own research purposes after anonymising or pseudonymising it and implementing the safeguards set out in Arts. 5(1)(b) and 89(1), GDPR and relevant provisions of Data Protection Law.

6. PROCESSING INSTRUCTIONS

6.1. Authority. You warrant that in cases where you are not sole Controller of any Protected Data (i.e. because you decide jointly with another Controller how and why to process Protect Data using the IIT or IIT Services), that you have full authority and authorisation of all relevant Controllers to provide Processing Instructions to us.

6.2. Only Authorised Users. It is your responsibility to ensure only Authorised Users provide Processing Instructions. You acknowledge and accept that if any Protected Data is deleted or improperly processed pursuant to Processing Instructions, we are under no obligation to seek to restore it and we assume no responsibility for such processing.

6.3. Providing Processing Instructions. Processing Instructions shall be considered to be provided where an Authorised User provides such instructions:

6.3.1. in writing, which may include but is not limited to email sent by an Authorised User, or

6.3.2. through configuration, selection or use of features, template elements, tools or other aspects of the IIT or by executing any computer command to process (including to delete) any Protected Data;

6.3.3. except to the extent any method in clause 6.3.2 is not fulfilled due to technical, operational or other reasons, in which case Processing Instructions will be deemed not to have been provided.

6.4. Limitation of Processor Liability. To the maximum extent permitted by mandatory law, we shall have no liability howsoever arising (whether in contract, tort (including negligence) or otherwise) for any losses, costs, expenses or liabilities (including any Data Protection Losses) arising from or in connection with any processing we do in accordance with your Processing Instructions, except where losses, costs, expenses or liabilities (including any Data Protection Losses) arise from our breach of this DPA (including but not limited to our breach of clause 5.2.3). For greater certainty, CWC shall be exempt from liability for Data Protection Losses under this paragraph 6.4 if it proves that it is not in any way responsible for the event giving rise to the damage.

7. DETAILS OF PROCESSING AND SECURITY

7.1. Details of Processing. Processing of Protected Data shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in the Annex A (Details of Processing) to this DPA.

7.2. Security. Taking into account the state of the art, the costs of implementation and the details of processing referenced in clause 7.1, as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons presented by the processing, we shall implement appropriate technical and organisational security measures in light of the risk, including those mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR.

7.3. Appropriate security. In light of the foregoing, we have determined that the measures set out in Annex B (Technical and Organisational Security Measures) to this DPA ensure a level of security appropriate to the risks of processing the Protected Data.

8. SUB-PROCESSING AND PERSONNEL

8.1. Prior authorisation. We shall only permit agents, subcontractors or other third parties to process Protected Data with your prior written authorisation (such authorisation not to be unreasonably withheld, conditioned or delayed), except with respect to our Sub-Processors' own employees in the course of their employment where those employees are subject to an enforceable obligation of confidence with regard to the Protected Data.

8.2. Authorised Sub-Processors. You authorise us to appoint each of the Sub-Processors identified in Annex C (List of Sub-Processors) as updated from time to time (following us obtaining ACE's prior written consent to any changes as required under the ACE Agreements). We shall provide reasonable notice of such updates and you will have the opportunity to object to such appointments.

8.3. We shall

8.3.1. appoint each Sub-Processor under a written contract containing materially the same obligations as under this DPA prior to any processing of Protected Data. Such contract shall be enforceable by us and we will ensure each such Sub-Processor complies with all such obligations;

8.3.2. remain fully liable for all the acts and omissions of each Sub-Processor as if they were our own to the extent that they relate to the data protection obligations under DP Law and this Agreement;

8.3.3. ensure that all natural persons authorised by us (or by any Sub-Processor) to process Protected Data are subject to a binding written contractual obligation of confidentiality (except where disclosure is required in accordance with Applicable Law, in which case we shall, where practicable and not prohibited by] Applicable Law, notify you of any such requirement before such disclosure).

9. ASSISTANCE AND DATA SUBJECT RIGHTS

9.1. We shall:

9.1.1. Security obligations and breach response. Assist you in ensuring compliance with your obligations pursuant to Articles 32 to 36 of the GDPR (Security of Personal Data and Data Protection Impact Assessments) and any similar obligations under applicable Data Protection Laws taking into account the nature of the processing and the information available to us; and

9.1.2. Data Subject Rights (DSRs). Taking into account the nature of the processing, assist you (by appropriate technical and organisational measures), insofar as this is possible, in fulfilling your obligations to respond to requests for exercising the Data Subjects' Rights under Chapter III of the GDPR (and any similar obligations under applicable Data Protection Laws) in respect of any Protected Data.

10. INTERNATIONAL DATA TRANSFERS

10.1. Adequacy and Standard Contractual Clauses. We shall not process and/or transfer, or otherwise directly or indirectly disclose, Protected Data in or to countries outside the United Kingdom or the EEA or to any International Organisation unless Appropriate Safeguards are in place. We undertake to minimise the amount of Protected Data subject to International Data Transfers and have implemented the Appropriate Safeguards described in Annex A (Details of Processing) and listed in Annex C (List of Sub-Processors) to this DPA as applicable.

10.2. Limitation. You acknowledge that due to the nature of cloud IIT, Authorised Users may initiate International Data Transfers of Protected Data to other geographical locations in connection with the use of the IIT. You acknowledge that we do not control such processing and you shall ensure that Authorised Users (and all others acting on your behalf) only initiate such transfers where Appropriate Safeguards are in place.

11. AUDITS AND PROCESSING

11.1. We shall, in accordance with DP Law, make available to you such information that is in our possession or control as is necessary to demonstrate our compliance with our obligations under this DPA and to demonstrate compliance with the obligations on each Party imposed by Article 28 of the GDPR (and under any equivalent Data Protection Laws equivalent to that Article 28), and allow for and contribute to audits, including inspections, by you (or another mutually agreed auditor) at your sole cost for this purpose (subject to a maximum of one audit request in any 12 month period). Any costs arising in connection with this clause 11.1 shall be reasonable and notified in advance by us to you and chargeable only where pre-agreed in writing.

12. BREACH

12.1. We shall notify you without undue delay and in writing on becoming aware of any Personal Data Breach in respect of any Protected Data.

13. DELETION/RETURN

13.1. Upon termination of the IIT, at your cost and your option, we shall either return all of the Protected Data to you or securely dispose of the Protected Data (and thereafter promptly delete all existing copies of it) except to the extent that any Applicable Law requires or permits us to store or continue to process such Protected Data. CWC reserves the right, on behalf of ACE, to retain Mandated Data, which does not include Personal Data. This clause shall survive termination or expiry of the Agreement or this DPA.

14. INDEMNITIES

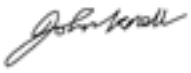
14.1. You shall indemnify us and keep us indemnified against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to Data Subjects, demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a Supervisory Authority), including all Data Protection Losses arising out of or in connection with any breach by you of your obligations under this DPA.

14.2. We shall indemnify you and keep you indemnified against all losses, claims, damages, liabilities, fines, sanctions, interest, penalties, costs, charges, expenses, compensation paid to Data Subjects, demands and legal and other professional costs (calculated on a full indemnity basis and in each case whether or not arising from any investigation by, or imposed by, a Supervisory Authority), including all Data Protection Losses arising out of or in connection with any breach by us of our obligations under this DPA.

15. DATA PROTECTION CONTACT

15.1. Our data protection lead is John Knell. He may be contacted via email at john@john-knell.com.

By signing below I warrant and represent that I am duly authorised to sign the Agreement and bind my organisation

For:	For Counting What Counts
Signature:	Signature: 
Title:	Title: Director
Date:	Date: 18-05-19

ANNEX A
DETAILS OF PROCESSING

Processing of the Protected Data by us under this DPA and the Agreement shall be for the subject-matter, duration, nature and purposes and involve the types of Personal Data and categories of Data Subjects set out in this Annex A based on the expected use of the IIT and IIT Services by NPOs and ACE, as applicable.

As a Controller, you and your Authorised Users decide which questions to use, how to design your Surveys, what Personal Data to process and why. We simply provide the IIT and IIT Services to enable you to do so. The details of processing will vary according to such choices but are generally described below based on our expected use of the IIT by NPOs.

Brief description of processing	NPOs can use the self-serve platform to create Surveys that capture questions prescribed by ACE or bespoke questions in order to gain audience insights. NPOs can generate reports and metrics. NPOs will receive training and have access to a help line and live support as well as access to training and demonstration videos.
What processing is being done? The following processing activities will primarily be performed by you in your capacity as Controller. Certain activities (marked with **) reflect where CWC processes the same data as a Controller for business administration purposes as described in our Data Privacy Notice https://impactandinsight.co.uk/cookie-policy	✓ Collection of Personal Data supplied by NPO and derived from IIT Use**. ✓ Storage/organisation ✓ Transfer outside the EEA to Australia. Our AWS server is in London but CC employees based in Australia process a limited amount of Protected Data (e.g. to provide support) as well as for CWC's own purposes as a Controller. CC developers in India and the US do not process any data. If in an exceptional case they needed to process Protected Data (for example to de-bug), which is unlikely, they would seek and document explicit consent of the Data Subject as required Art. 49(1)(a), GDPR. ✓ Use/consultation ✓ Transfer to a third party: see Annex C (List of Sub-Processors) ✓ Adaptation/alteration ✓ Retention ✓ Destruction/erasure / pseudonymisation / anonymisation ✓ Disclosure/dissemination Processing that will NOT be done: ✓ Combination/alignment (only anonymous elements of raw data captured will be aggregated for metrics purposes)
What types of data are being processed on behalf of NPO?	Participant Survey Data: the platform and Survey templates are designed to be anonymous or pseudonymous (in the case of Peer or Self Surveys) to minimise that amount of Survey Participant Personal Data that is visible or accessible to CWC and its Sub-Processors. You are encouraged to use the functionality and training provided to prevent Personal Data of Survey Participants from being transmitted to or accessible by us. The fields you select, and in particular bespoke questions you create and qualitative responses you receive may result in a Survey Participant becoming identifiable. Note also that in certain cases a full Postal Code or distinct data elements matched or cross-referenced may result in a Survey Participant becoming identifiable, making this Personal Data if you do not take appropriate steps to maintain anonymity, particularly if our recommendations are not followed or the functions we provide to reduce this risk are not enabled.

Authorised User Personal Data:

- Data provided by or on behalf of Authorised Users: email address; name; title; NPO; phone number; email address; help query; record of support provided; voice recording (for quality assurance and training purposes; Feedback (if you elect not to keep it anonymous); IIT Account permissions or privileges; Processing Instructions.

- Data derived from an Authorised User's interaction with the IIT or IIT Services: training and workshop logs confirming attendance in-person or online (and metadata associated with it, e.g. electronic time stamp, video analytics for videos viewed); login details and times; audit trails; cookie data (essential cookies). See our Data Privacy Notice https://impactandinsight.co.uk/privacy-policy/ for more detail.

Are cookies and other tracking tools used?

In connection with the IIT, we use cookies and other tracking technologies that are necessary to ensure our Platform function properly, e.g. to ensure the page remembers data entered when users move from question to question. For more detail see our Cookie Notice https://impactandinsight.co.uk/cookie-policy/.

Note: You shall provide Participants with an appropriate Data Privacy Notice related to the processing of cookie data and a means (e.g. a cookie dashboard, links to settings, etc.) to enable them to opt into cookies (where prior consent is required under Data Protection Law) and/or manage their preferences.

Sensitive data

The Platform is self-serve, so Authorised Users decide what types of Personal Data to collect, and this may include data that is sensitive and requires additional safeguards and requirements, including:

- Special Category data whose processing is restricted under Art. 9, GDPR and related Data Protection Law, such as health, ethnicity, political opinion;
- Criminal Records data, which is restricted under Art. 10,
- Financial data
- Location data

It is your responsibility as a Controller to ensure that if you do wish to process the types of data above you

- Consider the potential risk of harm to the individuals concerned;
- Take steps to mitigate those risks, including notably pseudonymisation if anonymisation is not possible or is unduly onerous; and
- you will fulfil any additional requirements (e.g. obtain explicit consent to process health data).

You may use the functionality and IIT features we provide in the IIT and best practices we address through IIT Services to help mitigate these risks.

Participant Survey Personal Data and Authorised User Personal Data you

	manage:
Duration of processing	You determine the duration and frequency of Surveys using the settings and features within the IIT. Participant Data and Authorised User Data that you manage using our IIT Account: will remain in your account until you delete or destroy it. Authorised User Personal Data and Derived Personal Data**: See our Data Privacy Notice for details https://impactandinsight.co.uk/privacy-policy/
How is the processing being done?	Protected Data is processed using various self-serve options initiated by you or Authorised Users to send or process Surveys or other data, and we also assist on the back-end of the Platform and in our interactions with you as follows:
Why is the processing being done?	To enable NPO to understand the audiences they attract to their shows, benchmark performance, and engage with Participants to get better insights.
Who is the data about?	Participants, Authorised Users, NPO (where NPO is a natural person). **Vulnerable People:** NPOs may decide (or be required) to conduct Surveys involving vulnerable people, such as children aged 13 or under, or people under protective supervision or who rely on a carer. In such cases Controllers have enhanced transparency obligations and additional consent requirements under DP Law may apply, e.g. consent of a parent or supervising adult. See e.g. ICO guidance. ico.org.uk We have provided functionality, training and support that you may find helpful in meeting these requirements. You are responsible for ensuring you take the necessary measures to meet these obligations.
What risks does the data processing pose to data subjects (if any)?	Any type of Personal Data Breach, including mis-handling or misuse of Protected Data beyond the purposes, e.g.: • Marketing under the guise of market research (for the survey functionality) without fulfilling marketing rules • Access by unauthorised individuals to Protected Data • Retaining Protected Data longer than necessary • Processing Children's Personal Data or communicating with children without appropriate protections
What mitigating measures are being taken to address those risks?	• NPO is responsible for ensuring use of IIT complies with DP Law. • CWC has implemented various controls and security measures (see Annex B to this DPA), e.g. personnel have limited access to insights data and are bound by confidentiality which includes a commitment not to use Protected Data for their own purposes.

	• The IIT includes optional functionality that Authorised Users can use to address these risks. • CWC provides ongoing training and support in how to use the IIT and IIT Services and which incorporates data protection tips and best practices using the IIT. • See Annex B for related measures.
Is the Protected Data being transferred outside of the EEA? If so, describe the Adequate Safeguards you have implemented.	Yes. The CC Platform is operated from Australia, but the server is hosted in London. We are taking steps to minimise the amount of Protected Data that is transferred outside of the EEA but since we cannot guarantee none will be transferred we have prepared Standard Contractual Clauses for you to sign with CC, which form part of your contractual package and this Agreement. Should you wish to obtain a copy of these Contractual Clauses due to the loss of your provided copy, please contact support@countingwhatcounts.co.uk See also Annex B for additional measures we have taken.

ANNEX B

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

1. We shall implement and maintain the following technical and organisational security measures to protect the Protected Data In accordance with DP Laws:

(a) taking into account the state of the art, the costs of implementation and the Details of Processing and the risks of varying likelihood and severity for the rights and freedoms of natural persons and the risks that are presented by the processing;

(b) implementing appropriate technical and organisational security measures appropriate to the risk, including as appropriate those matters mentioned in Articles 32(1)(a) to 32(1)(d) (inclusive) of the GDPR and relevant provisions of applicable DP Law and as spelled out in more detail in the chart below;

(c) regularly reviewing and updating the measures in order to achieve compliance with this clause in light of developments in technology, security and methods of deliberate attack on computer systems and the factors listed in clauses 1.1 and 1.2;

2. You acknowledge that none of the below measures relieves you of your own obligations under DP Law, notably Arts. 24 (Responsibility of the Controller), 25 (Data Protection by Design and Default), and 32-34 (Security of Processing), 35-36 (Data Protection Impact Assessments).

3. You warrant and represent that you will not in any way undermine, disable, interfere with or otherwise circumvent the above measures. This includes, but is not limited to, attempting to re-identify data that has been de-identified, which is prohibited under DP Law.

4. Details of Technical and Organisational Security Measures are:

	TYPE OF MEASURE	DESCRIPTION
	EXTERNAL CERTIFICATIONS	
1	Information security management certifications/accreditations, other certifications, codes of conduct, trust marks or seals	We adhere to the principles of ISO27001. We also conform to the Cyber Essentials Framework and are working towards certification.
	RISK ASSESSMENT, SECURITY CLASSIFICATION OF INFORMATION, END-USER DEVICES AND TESTING	
2	Ongoing risk assessments	• At least twice per year we methodologically go through points of stack, identify vulnerabilities and establish a risk matrix which includes possible impacts to various Data Subjects by user category (e.g. survey participant, organisation, Authorised User, staff, developer). Then identify mitigations, establish an action list, and consider possible impacts post-mitigation. • We continuously scan the environment and the threat landscape to identify environmental or episodic risks which trigger a review of the whole risk profile and appropriate changes to the risk framework. Feedback loops and 'near misses' continuously inform our risk profile.
3	Testing and monitoring	• We run pre-deployment vulnerability assessments. We regularly run test suites internally. We write tests and run them whenever we deploy new code to ensure there aren't any broken spots in the system. We also run synthetic tests. • Our monitoring suite includes data leakage protection, bandwidth logs and alerts, IP address logs. • Our platform undergoes regular penetration and vulnerability tests by external parties. The next penetration test is scheduled for mid-April 2019 shortly after the Go Live date. • Our Windows and SQL servers are frequently tested and undergo regular security updates and patches. • We also run internal vulnerability assessments. including mock disaster recovery at regular intervals. • We require our developers to comply with internal coding standards that align with best practices.

4	Patches and updates	• We regularly patch and run software updates. • The software is built entirely on open-source tech and we ensure all COTS tech remains within mainstream support.
5	Business continuity measures are in place to provide protection against equipment failure or damage and are tested regularly.	• System is backed up regularly with rolling backups to ensure purposefully removed data is not present in backups. • We have disaster recovery procedures in place to ensure integrity of backups. • NOTE: backups are retained for 6 months only.
6	Controls to prevent human error such as accidental deletion or alteration are in place.	• Data can only be completely deleted by a Super-User. Prompts are in place to minimise risk of accidental deletion. • Edits to Survey response data require manual saving to prevent accidental changes.
7	Audit	• We periodically run internal audits. We maintain and review audit logs. • Annual external audits are planned.
8	Security classification of information	• We have identified different data types and implemented controls to address varying risks, e.g. fields that may contain identifiable data within Protected Data is segregated or hashed where possible to minimise the amount of Personal Data accessible by or processed by us. • Fields that may contain Special Categories of Data are treated differently and in any case we reduce the likelihood of the data being accessible by us. • We distinguish Mandated Data from Protected Data and adjust access controls accordingly.

NETWORKING, END-USER DEVICES, ENCRYPTION

9	Segregation / Isolation	• CC UK has its own standalone server. We have extracted UK-based trial data from the Australian server and created a web node in the UK with a UK-based server in London to ensure NPO / ACE data is completely isolated from other CC client data.
10	End-User Devices containing NPO data	• It is very unlikely that personnel using mobile devices would use them for Protected Data, Mandated Data or other data belonging to either NPOs or ACE. If so, this would be ad hoc. The developers use mobile or personal devices to write code and debug, not to process data. • The low likelihood of this occurring and the access controls described below make it unnecessary to encrypt mobile devices.

11	Personal data is securely encrypted when stored and when transferred.	• Emails are encrypted in transit (SASL uses TSL for encryption) • Email addresses are obscured in logs • Customer accounts are protected by encrypted passwords • All data travels on Digital Ocean private networks. There are technical and procedural measures to reduce the risk of rogue Digital Ocean personnel to read or access data in transit between the server and the web node. For detail see: https://www.digitalocean.com/legal/data-security/ + https://www.digitalocean.com/legal/privacy-policy/ • NOTE: we minimise the amount of Personal Data transferred to our database to reduce risk.

PERSONNEL SECURITY, PHYSICAL SECURITY, ACCESS CONTROLS, DATA DELETION / DESTRUCTION

12	Physical security controls to prevent unauthorised access, theft or damage to physical equipment.	• Our system is stored on a Server Farm operated by Digital Oceans which implement a number of physical and other security measures. More detail here: https://www.digitalocean.com/legal/data-security/. • Our server cabinet is physically secured and only specific, authorised people may gain access to it. • We have procedures in place to ensure data is removed from computer machines when it is no longer needed • We use passcards, physical locks, safe and other physical controls in the office.
13	Staff reliability checks are carried out when recruiting.	• Employer reference checks on all staff. • Staff sign confidentiality agreements and those who process Protected Data are made aware of their responsibilities under DP Law (see Governance and Training, below)

14 Access Controls

*Note: we have limited the amount of Protected Data that is processed on our systems as described below.

Granular access controls are in place and access to Protected Data is limited to staff who need to have access to carry out legitimate tasks, notably:

- Developers have root access only to databases on which they work. Super-Users have access to all databases but do not have root access. Super-User dictates a range of permission levels. The NPO administrator can grant Authorised Users permission to use the dashboard, e.g. to access survey or report and can set functional permissions as well (e.g. read-only, edit). Survey Participants have access to complete the survey but cannot see data of other Survey Participants.

- Customer account is protected by an encrypted password. Only Support Staff and a limited number of Super-Users have access to Customer accounts and Protected Data;

- Such access is granted only with Customer's express permission, triggered only when a support ticket has been opened and Customer has affirmatively provided access.

- Exception: a limited number of Super-Users may access to Customer Accounts to resolve an alert.

- Customers may choose to share data using the in-built sharing systems with staff for production of reporting outputs and are advised to be wary of sharing sensitive data before this occurs. We have procedures in place to prevent unnecessary data sharing including hashing Survey response data within Protected Data fields like email.

- Our production system is segregated from our staging system. Developers use data fixtures designed to test. Real data may be used in certain cases where issues cannot be replicated by use of fixtures, where there is a low risk of encountering Protected Data and only with that Customer's express permission (as above).

- Support staff may gain access to certain Protected Data and, in such cases, only incidentally in the course of providing technical support. We keep and review audit logs.

15 Data deletion / destruction

- We back data up on a rolling basis. Data deleted from the database will remain in back-up until the 6-month retention period has passed. A regular administrative user or end-user cannot delete from the back-up. Only a Super-User can.

- Retain the data for 6 months

ORGANISATIONAL MEASURES AND OTHER CONTROLS

16	Governance	• We have implemented appropriate information security policies and procedures in line with ISO 27000 and the Cyber Essentials framework including: • Procedures to regularly review data access rights. • Procedures for the secure disposal of data, media and equipment. • Procedures to regularly review our risk exposure and table appropriate mitigations that consider possible impact on customers and end-users, best practice solutions, and resource availability. • Internal Data Protection and Information Security policy documents are being updated for employees to align with Data Protection Law requirements and employees will be trained on their corresponding obligations.
17	Staff are trained on information security, confidentiality and data protection.	• All staff undergo periodic data protection and IT security training. • New employees undergo comprehensive induction programmes inclusive of the above subject matter. • Staff sign legally-binding confidentiality agreements and are made aware that any re-purposing or use of Protected Data and any Personal Data we process for our own purposes as a Controller is strictly prohibited.
18	Data-minimisation	• Surveys are designed to be anonymous (or pseudonymous where re-linking may be required). • Survey responses to email-type inputs can only be viewed by the creator of an evaluation, and are obscured for other users. • Customers are warned about the risks of collecting personal data through surveys they create through various training materials.
19	Data Subject Rights and Preference Management	• Customers can correct, delete or export in common machine-readable format any data elements they have inputted the forms in Customer accounts to help fulfil erasure, rectification, portability or access requests with assistance of support staff.
20	Secure architecture	• The Platform and IIT Services are designed in accordance with NCSC “Security Design Principles for Digital Services”, “Bulk Data Principles”, and “Cloud Security Principles”

ANNEX C
LIST OF SUB PROCESSORS

This is where we maintain a current List of Sub-Processors authorised to process Protected Data. We impose data protection terms on each Sub-Processor regarding their technical and organisational measures or the protection of Personal Data and applicable DP Laws.

ENTITY NAME	ENTITY TYPE & PROCESSING ACTIVITY	ENTITY LOCATION	ADEQUATE SAFEGUARD (if transferred outside EEA)
EXTERNAL CERTIFICATIONS			
Culture Counts Pty (CC)	Software as a Service Platform and analytics service for surveys. Note: We have minimised the amount of Protected Data that might be accessed by CC employees in Australia. In rare cases of technical escalation they may require such access upon NPO request. CC employees will process a minimum amount of Authorised User data as described in clause 1.1.4(14)(Access Controls) of this Annex B.	Australia	Standard Contractual Clauses (Annex A, Part 2)
Digital Ocean	VPS machines: • web-uk-1: application stack web node • web-uk-2: application stack web node • database-uk: database for application • backup-uk: holds database snapshots of uk database • cache-uk: Stores sessions and application 'objects' in RAM for the webnodes Load Balancer: uk.culturecounts.cc directs incoming traffic to the two web nodes	London	NA

Docusign	e-Signature Provider (for NPO signatures)	US (California)	Binding Corporate Rules for Processors available here.
S3 - Amazon	Media files (uploads) / static assets	London	N/A

ANNEX D

RECOMMENDED PROCESSOR PRIVACY STATEMENTS (FAQS)

1. Purpose. These recommended statements are optional and intended to make it easier for you to communicate privacy information to your Participants concerning our role in processing Protected Data on your behalf. This does not relieve you of your obligation to provide a full Data Privacy Notice to your Participants or others.

2. Restriction. You may not modify the content without our prior, written consent and approval of the new proposed text.

3. Recommended Processor Privacy Statements. We have provided three optional statements:

a. High-Level Statement. A high-level statement by you that you may include in your own Data Privacy Notice:
We use CWC https://countingwhatcounts.co.uk as our Processor to power our Surveys and Participant Communications with you. We have signed a legally-binding agreement with NPO and ACE confirming it will only collect and store information about you according to our instructions, based on how we use their self-serve platform. CWC has taken steps to minimise the amount of personal data it can see or access when processing on our behalf and to make sure its appropriately secured.
See the CWC Privacy Policy

b. Cookies Statement.
Cookies: CWC places 'cookies' or other trackers on your device that are necessary to make sure our Communications run smoothly as described in their Cookie Notice https://impactandinsight.co.uk/cookie-policy/. They also process some data for their purposes as a Controller. See their Data privacy Notice for more https://impactandinsight.co.uk/privacy-policy/

c. CWC Processor Privacy FAQs. You may link to this document to provide your Participants with more information about how we help you process Protected Data:

What is this and who should read this?
This is intended to answer questions you may have if you've received communication sent to you related to our platform. If you wish to know about our practices when you visit our site directly or engage directly with us, please see our Data Privacy Notice https://impactandinsight.co.uk/privacy-policy/

What is CWC and what are you doing with my data?
CWC is the provider of our Survey platform. When NPOs use our platform to deliver surveys to you, they select the types of data to capture about you by selecting the questions. Our NPO decides what to do with it. This will vary with each NPO. We just support our NPO by collecting, transmitting and securely storing your personal data in their private NPO account (which is protected with an encrypted password) and providing support when necessary. We do not deliberately access, see, use or otherwise benefit from this information, though a member of our support team

may incidentally see some account content while providing NPO support.

Does CWC do anything else with my data?
No. In GDPR terms, we're the data processor for most of what we do with your personal data, and our NPO is the data controller. There are certain situations where we act as a Controller and use a limited about of your personal data for our purposes. See **Does CWC ever use my data for its own purposes?** below**.**

As a data processor, we only process your personal data according to our NPO's instructions and only process or view what is necessary to enable our NPOs to use the platform. We provide the platform on a self-serve basis with templates and functionality that the NPO uses to communicate with you and capture your personal data. This includes optional information to confirm delivery.

Within CWC we have controls in place to enforce need-to-know access and our employees are bound by strict confidentiality obligations. The same applies to our sub-processors. Where we do gain access, only personnel with a legitimate need-to-know will have that access for support purposes. Our personnel are bound by confidentiality, and we are contractually obligated to process your data only on our NPOs' instructions and in a secure manner. [See Schedule II (Data Protection Addendum) (DPA) supplied as part of your contractual package, in particular Annex A (Details of Processing) and Annex B (Technical and Organisational Security Measures)

If you have other entities who use your platform to capture my details in their own accounts, do you ever combine my information from different NPO accounts or allow others to so they can create richer profiles of me or track me across all these platforms?

No. We never mingle Personal Data across NPO accounts, although individual NPOs may elect to use the share function to share some of their data with other NPOs. The NPO(s) whose survey(s) you have completed will be able to provide you with that information.

We don't use the Personal Data they input into our platform for our own use. However, with our Client's prior written approval we may anonymise or pseudonymise aggregated data we process for our own research purposes and we may match such anonymised data sets with other public data strictly for research purposes. **We will only do so in accordance with Data Protection Law, specifically as provided under Arts. 5(1)(b) and 89(1), GDPR and relevant Data Protection Law, and after considering and mitigating risks of re-identification.**

How can I manage my privacy settings?
Our NPO, as the data controller, ultimately decides how to respond to privacy rights requests, like requests for information about what data our NPO holds on you, or requests to erase your data. CWC only processes a portion of the personal data our NPO may have about you. Please contact the relevant NPO if you wish to exercise your privacy rights.

ANNEX E
(DATA PROTECTION GUIDANCE)

The Parties acknowledge and agree that this Annex E is not legally binding and is for NPO guidance only.

(a) Lawful Collection and Processing. You confirm that:

(i) Protected Data shall be collected lawfully and, where it is collected indirectly, you have undertaken the necessary due diligence to confirm you are permitted to process it;

(ii) that you have documented a valid lawful basis for processing the Protected Data according to your Processing Instructions, and in particular with respect to special categories of data or sensitive data as listed in Arts. 9 and 10, GDPR; and

(iii) that you maintain evidence to demonstrate such lawful basis exists. This includes, where consent is required or selected, obtaining and documenting all necessary consents to the different processing activities you undertake using the IIT or in the Processing Instructions and ensuring that these will remain valid at all times.

(iv) Accuracy. Protected Data is and will remain accurate and up to date.

(v) Storage (Data-Retention). Protected Data will only be stored in the IIT for as long as necessary to satisfy the processing purposes.

(b) Security. You shall establish and maintain adequate security measures to:

(i) safeguard Protected Data in your possession or control from unauthorised access and copying and maintain complete and accurate backups of all Protected Data provided to us (or anyone acting on our behalf) so as to] be able to immediately recover and reconstitute such Protected Data in the event of loss, damage or corruption; and

(ii) ensure Participant Communications or other use of the IIT does not contain or transmit spyware, viruses, worms, trojan horses, adware or other malware, or expose our IIT, the Participants or the devices of other Data Subjects to such programs in an indirect way.